Cybersecurity
PAST TENSE

Simple past tense : we use the past to talk about actions that began and finished in the past.

- The security team detected a phishing attempt in the email system.
- Hackers breached the company's firewall last month.
- The IT department implemented new encryption protocols to protect sensitive data.
- They analyzed the malware and identified its origin.
- The organization conducted a thorough vulnerability assessment.
- Employees completed cybersecurity training to recognize potential threats.
- The software updated automatically to patch known security flaws.
- Cybercriminals exploited a weakness in the application’s code.
- The incident response team contained the breach within hours.
- The company reported the data leak to regulatory authorities.

Simple past sentences

- Cybercriminals launched ransomware attacks that encrypted files and demanded payment for their release.
- Malware, including viruses and worms, infected numerous systems and caused significant data loss.
- Attackers exploited vulnerabilities in software through SQL injection attacks, which allowed them to access sensitive databases.
- Distributed Denial-of-Service (DDoS) attacks overwhelmed networks, rendering them inaccessible to legitimate users.
- Man-in-the-middle attacks intercepted communications between two parties without their knowledge, leading to data theft.
- Crypto jacking incidents hijacked computer resources to mine cryptocurrency without the owners' consent.

Negative sentences in the past : we use the Word didn´t to change the meaning in the neative form. We don´t change the verb.

- Data Breach: The company did not recover from the data breach that exposed sensitive customer information.
- Malware: The organization did not fail to detect the malware before it compromised their entire network.
- Phishing Attack: Many employees did not recognize the phishing attack and inadvertently provided their login credentials.
- Firewall: The firewall did not prevent unauthorized access, leading to a significant security incident.
- Encryption: The sensitive files were not encrypted, making them vulnerable to interception during transmission.
- Ransomware: They did not have a backup solution in place when the ransomware attack occurred, resulting in permanent data loss.

Simple past negative sentences

- Vulnerability: The team did not patch the vulnerability in time, allowing hackers to exploit it successfully.
- Incident Response: The incident response plan was not executed properly, causing delays in addressing the security breach.
- Two-Factor Authentication (2FA): The users did not enable two-factor authentication, which could have prevented unauthorized access to their accounts.
- Cybersecurity Training: Employees did not participate in the cybersecurity training, leaving them unprepared for potential threats.

Yes/no questions in the simple past tense

- Did the team implement two-factor authentication last month?
- Did you encrypt the sensitive data before sending it?
- Did you implement two-factor authentication for all users recently?
- Did you discover any vulnerabilities during your latest security scan? Did the organization implement a firewall last year?
- Did the IT team conduct a vulnerability assessment before the attack?
- Did employees receive cybersecurity training before the phishing incident?
- Did the company back up its data regularly in the past year?
- Did the security incident response team respond promptly to the breach?
- Did you ever encounter a phishing attack
- Did you use strong passwords always
- Did you ever report a cybersecurity incident

Making information questions in the past tense

- What did you discover during the security audit?
  I discovered several vulnerabilities in the network systems.
- What steps did you take after you identified a security breach?
  I isolated the infected systems and notified the relevant authorities.
- When did you last update the firewall settings?
  I updated the firewall settings two weeks ago.
- What measures did your organization take to prevent phishing attacks?
  We conducted training sessions and implemented email filtering systems.
- How did you manage cryptographic keys in your last project?
  I generated, stored, and rotated cryptographic keys securely throughout the project.

Information questions and answers

- Where did you find the malware during your investigation?

  I found the malware in an unpatched software application on a server.

- Why did you choose to use a VPN for remote access?

  I chose to use a VPN to secure the connection and protect sensitive information.

- What challenges did you face during the disaster recovery process?

  We faced challenges with data restoration and system compatibility during recovery.

Regular verbs pronunciation in the past /ed/

- VALIDATE RECOGNIZE PROVIDE ENCRYPT OCCUR EXECUTE
- REQUIRE PREVENT PREPARE EXPLOIT ATTACK DELAY
- AVOID BREACH DISGUISE ALLOW ACCESS COMPROMISE
- FACE INCLUDE AFFECT STORE INVOLVE CREATE
- FAIL USE OPEN CLOSE CONCERN ASSOCIATE
- ATTEMPT COMPLEMENT DETECT IDENTIFY ANALYZE COMPLETE
- EXPOSE UPDATE REPORT LAUNCH INTERCEPT HIJACK
- EXECUTE PARTICIPATE RECEIVE ENCOUNTER DISCOVER ROTATE